

PCT

NOTIFICATION OF ELECTION

(PCT Rule 61.2)

From the INTERNATIONAL BUREAU

To:

Assistant Commissioner for Patents
United States Patent and Trademark
Office
Box PCT
Washington, D.C.20231
ETATS-UNIS D'AMERIQUE

in its capacity as elected Office

| | |
|--|--|
| Date of mailing (day/month/year) 16 October 2000 (16.10.00) | |
| International application No. PCT/US00/02317 | Applicant's or agent's file reference 18926-34PC |
| International filing date (day/month/year) 28 January 2000 (28.01.00) | Priority date (day/month/year) 29 January 1999 (29.01.99) |
| Applicant MEDVINSKY, Sasha et al | |

1. The designated Office is hereby notified of its election made:

☒ in the demand filed with the International Preliminary Examining Authority on:
22 August 2000 (22.08.00)

☐ in a notice effecting later election filed with the International Bureau on:

2. The election ☒ was
☐ was not

made before the expiration of 19 months from the priority date or, where Rule 32 applies, within the time limit under Rule 32.2(b).

| | |
|---|---|
| The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland Facsimile No.: (41-22) 740.14.35 | Authorized officer J. Leitao Telephone No.: (41-22) 338.83.38 |
|---|---|

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

REC'D 22 JUN 2001

WIPO

PCT

| | | |
|---|---|---|
| Applicant's or agent's file reference 18926-34PC | FOR FURTHER ACTION See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416) | |
| International application No. PCT/US00/02317 | International filing date (day/month/year) 28 JANUARY 2000 | Priority date (day/month/year) 29 JANUARY 1999 |
| International Patent Classification (IPC) or national classification and IPC IPC(7): H04L 9/32; G06F 17/60 and US Cl.: 713/168, 175, 200, 201, 202 | | |
| Applicant GENERAL INSTRUMENT CORPORATION | | |

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.
2. This REPORT consists of a total of 3 sheets.
☐ This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority. (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).
These annexes consist of a total of 0 sheets.
3. This report contains indications relating to the following items:
 - I ☒ Basis of the report
 - II ☐ Priority
 - III ☐ Non-establishment of report with regard to novelty, inventive step or industrial applicability
 - IV ☐ Lack of unity of invention
 - V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
 - VI ☐ Certain documents cited
 - VII ☐ Certain defects in the international application
 - VIII ☐ Certain observations on the international application

| | |
|--|---|
| Date of submission of the demand 22 AUGUST 2000 | Date of completion of this report 15 MAY 2001 |
| Name and mailing address of the IPEA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230 | Authorized officer THOMAS C. LEE <i>James R. Matthews</i> Telephone No. (703) 305-9717 |

I. Basis of the report**1. With regard to the elements of the international application:***

- ☒ the international application as originally filed
- ☒ the description:
pages 1-9 , as originally filed
pages NONE , filed with the demand
pages NONE , filed with the letter of _____
- ☒ the claims:
pages 10 , as originally filed
pages NONE , as amended (together with any statement) under Article 19
pages NONE , filed with the demand
pages NONE , filed with the letter of _____
- ☒ the drawings:
pages 1-3 , as originally filed
pages NONE , filed with the demand
pages NONE , filed with the letter of _____
- ☒ the sequence listing part of the
description: NONE , as originally filed
pages NONE , filed with the demand
pages NONE , filed with the letter of _____

2. With regard to the language, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.

These elements were available or furnished to this Authority in the following language _____ which is:

- ☐ the language of a translation furnished for the purposes of international search (under Rule 23.1(b)).
- ☐ the language of publication of the international application (under Rule 48.3(b)).
- ☐ the language of the translation furnished for the purposes of international preliminary examination (under Rules 55.2 and/or 55.3).

3. With regard to any nucleotide and/or amino acid sequence disclosed in the international application, the international

- ☐ contained in the international application in printed form.
- ☐ filed together with the international application in computer readable form.
- ☐ furnished subsequently to this Authority in written form.
- ☐ furnished subsequently to this Authority in computer readable form.
- ☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.
- ☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. ☒ The amendments have resulted in the cancellation of:

- ☒ the description, pages NONE
- ☒ the claims, Nos. NONE
- ☒ the drawings, sheets/fig NONE

5. ☐ This report has been drawn as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).**

*** Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rules 70.16 and 70.17).**

****Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.**

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.

PCT/US00/02317

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement**1. statement**

| | | | |
|-------------------------------|--------|-------------|-----|
| Novelty (N) | Claims | <u>1-2</u> | YES |
| | Claims | <u>NONE</u> | NO |
| Inventive Step (IS) | Claims | <u>NONE</u> | YES |
| | Claims | <u>1-2</u> | NO |
| Industrial Applicability (IA) | Claims | <u>1-2</u> | YES |
| | Claims | <u>NONE</u> | NO |

2. citations and explanations (Rule 70.7)

Claims 1 and 2 lack an inventive step under PCT Article 33(3) as being obvious over Austin, US patent No. 4,935,962 in view of Fischer, US patent No. 4,868,877.

As per claim 1, Austin teaches a method for providing self-issuing certificates (col. 11, lines 42-44) in a device (card 30), the method comprising:

receiving, from an external source (card acceptor device 32) a request to generate a new certificate, wherein the request includes (col. 8, lines 5-6) an encrypted public key (public key e);

using a secure microprocessor (microprocessor 36) to generate a new certificate(Y) that uses (col. 8, lines 11-13) the public key; and

using the new certificate in data transfers (col. 8, lines 30-33).

However, Austin does not teach the device in a telecommunication system.

Fischer teaches a device (terminal A) in a telecommunication system (col. 5, lines 60-65).

Therefore, it would have been obvious to one of ordinary skill in the art to combine the teachings of Austin and Fischer because they both teach a data transfer using a certificate and the Fischer's teaching of application in telecommunication system would increase flexibility in Austin's data communication path (data communication path 34).

As per claim 2, Fischer teaches a validity time (expiration date in fig. 5) in a new certificate.

----- NEW CITATIONS -----

US 4,935,962 A (AUSTIN) 19 June 1990, see abstract, col. 7, line 51-col. 8, line 34, col. 11, lines 35-48

US 4,868,877 A (FISCHER) 19 September 1989, col. 5, lines 60-65, fig. 5

PATENT COOPERATION TREATY

From the
INTERNATIONAL PRELIMINARY EXAMINING AUTHORITY

To: CHARLES J. KULAS
TOWNSEND AND TOWNSEND AND CREW LLP
TWO EMBARCADERO CENTER
EIGHT FLOOR
SAN FRANCISCO, CA 94111

PCT

NOTIFICATION OF TRANSMITTAL OF INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Rule 71.1)

Date of Mailing
(day/month/year)

19 JUN 2001

Applicant's or agent's file reference
18926-34PC

IMPORTANT NOTIFICATION

International application No.
PCT/US00/02317

International filing date (day/month/year)
28 JANUARY 2000

Priority Date (day/month/year)
29 JANUARY 1999

Applicant
GENERAL INSTRUMENT CORPORATION

1. The applicant is hereby notified that this International Preliminary Examining Authority transmits herewith the international preliminary examination report and its annexes, if any, established on the international application.
2. A copy of the report and its annexes, if any, is being transmitted to the International Bureau for communication to all the elected Offices.
3. Where required by any of the elected Offices, the International Bureau will prepare an English translation of the report (but not of any annexes) and will transmit such translation to those Offices.
4. **REMINDER**

The applicant must enter the national phase before each elected Office by performing certain acts (filing translations and paying national fees) within 30 months from the priority date (or later in some Offices)(Article 39(1))(see also the reminder sent by the International Bureau with Form PCT/IB/301).

Where a translation of the international application must be furnished to an elected Office, that translation must contain a translation of any annexes to the international preliminary examination report. It is the applicant's responsibility to prepare and furnish such translation directly to each elected Office concerned.

For further details on the applicable time limits and requirements of the elected Offices, see Volume II of the PCT Applicant's Guide.

Name and mailing address of the IPEA/US
Commissioner of Patents and Trademarks
Box PCT
Washington, D.C. 20231

Facsimile No. (703) 305-3230

Authorized officer

THOMAS C. LEE

James R. Matthews
Telephone No. (703) 305-9717

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

| | | |
|---|---|---|
| Applicant's or agent's file reference 18926-34PC | FOR FURTHER ACTION See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416) | |
| International application No. PCT/US00/02317 | International filing date (day/month/year) 28 JANUARY 2000 | Priority date (day/month/year) 29 JANUARY 1999 |
| International Patent Classification (IPC) or national classification and IPC IPC(7): H04L 9/32; G06F 17/60 and US Cl.: 713/168, 175, 200, 201, 202 | | |
| Applicant GENERAL INSTRUMENT CORPORATION | | |

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.
2. This REPORT consists of a total of 3 sheets.
☐ This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority. (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

These annexes consist of a total of 0 sheets.

3. This report contains indications relating to the following items:
 - ☒ Basis of the report
 - ☐ Priority
 - ☐ Non-establishment of report with regard to novelty, inventive step or industrial applicability
 - ☐ Lack of unity of invention
 - ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
 - ☐ Certain documents cited
 - ☐ Certain defects in the international application
 - ☐ Certain observations on the international application

| | |
|--|---|
| Date of submission of the demand 22 AUGUST 2000 | Date of completion of this report 15 MAY 2001 |
| Name and mailing address of the IPEA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230 | Authorized officer THOMAS C. LEE <i>James R. Matthews</i> Telephone No. (703) 305-9717 |

I. Basis of the report**1. With regard to the elements of the international application:***

- ☒ the international application as originally filed
- ☒ the description:
pages 1-9 , as originally filed
pages NONE , filed with the demand
pages NONE , filed with the letter of _____
- ☒ the claims:
pages 10 , as originally filed
pages NONE , as amended (together with any statement) under Article 19
pages NONE , filed with the demand
pages NONE , filed with the letter of _____
- ☒ the drawings:
pages 1-3 , as originally filed
pages NONE , filed with the demand
pages NONE , filed with the letter of _____
- ☒ the sequence listing part of the description:
pages NONE , as originally filed
pages NONE , filed with the demand
pages NONE , filed with the letter of _____

2. With regard to the language, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.

These elements were available or furnished to this Authority in the following language _____ which is:

- ☐ the language of a translation furnished for the purposes of international search (under Rule 23.1(b)).
- ☐ the language of publication of the international application (under Rule 48.3(b)).
- ☐ the language of the translation furnished for the purposes of international preliminary examination (under Rules 55.2 and/or 55.3).

3. With regard to any nucleotide and/or amino acid sequence disclosed in the international application, the international

- ☐ contained in the international application in printed form.
- ☐ filed together with the international application in computer readable form.
- ☐ furnished subsequently to this Authority in written form.
- ☐ furnished subsequently to this Authority in computer readable form.
- ☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.
- ☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. ☒ The amendments have resulted in the cancellation of:

- ☒ the description, pages NONE
- ☒ the claims, Nos. NONE
- ☒ the drawings, sheets/fig NONE

5. ☐ This report has been drawn as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).**

** Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rules 70.16 and 70.17).*

***Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.*

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.

PCT/US00/02317

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement**1. statement**

| | | |
|-------------------------------|-------------|-----|
| Novelty (N) | Claims 1-2 | YES |
| | Claims NONE | NO |
| Inventive Step (IS) | Claims NONE | YES |
| | Claims 1-2 | NO |
| Industrial Applicability (IA) | Claims 1-2 | YES |
| | Claims NONE | NO |

2. citations and explanations (Rule 70.7)

Claims 1 and 2 lack an inventive step under PCT Article 33(3) as being obvious over Austin, US patent No. 4,935,962 in view of Fischer, US patent No. 4,868,877.

As per claim 1, Austin teaches a method for providing self-issuing certificates (col. 11, lines 42-44) in a device (card 30), the method comprising:

receiving, from an external source (card acceptor device 32) a request to generate a new certificate, wherein the request includes (col. 8, lines 5-6) an encrypted public key (public key e);

using a secure microprocessor (microprocessor 36) to generate a new certificate(Y) that uses (col. 8, lines 11-13) the public key; and

using the new certificate in data transfers (col. 8, lines 30-33).

However, Austin does not teach the device in a telecommunication system.

Fischer teaches a device (terminal A) in a telecommunication system (col. 5, lines 60-65).

Therefore, it would have been obvious to one of ordinary skill in the art to combine the teachings of Austin and Fischer because they both teach a data transfer using a certificate and the Fischer's teaching of application in telecommunication system would increase flexibility in Austin's data communication path (data communication path 34).

As per claim 2, Fischer teaches a validity time (expiration date in fig. 5) in a new certificate.

----- NEW CITATIONS -----

US 4,935,962 A (AUSTIN) 19 June 1990, see abstract, col. 7, line 51-col. 8, line 34, col. 11, lines 35-48

US 4,868,877 A (FISCHER) 19 September 1989, col. 5, lines 60-65, fig. 5

PCTWORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

| | | |
|--|-----------|--|
| (51) International Patent Classification ⁷ : G06F | A2 | (11) International Publication Number: WO 00/45241 (43) International Publication Date: 3 August 2000 (03.08.00) |
| (21) International Application Number: PCT/US00/02317 (22) International Filing Date: 28 January 2000 (28.01.00) (30) Priority Data: 60/117,788 29 January 1999 (29.01.99) US 60/128,772 9 April 1999 (09.04.99) US (71) Applicant (for all designated States except US): GENERAL INSTRUMENT CORPORATION [US/US]; 101 Tounament Drive, Horsham, PA 19044 (US). (72) Inventors; and (75) Inventors/Applicants (for US only): MEDVINSKY, Sasha [US/US]; 8873 Hampe Court, San Diego, CA 92129 (US). SPRUNK, Eric, J. [US/US]; 6421 Cayenne Lane, Carlsbad, CA 92009 (US). (74) Agents: KULAS, Charles, J. et al.; Townsend and Townsend and Crew LLP, 8th floor, Two Embarcadero Center, San Francisco, CA 94111 (US). | | (81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG). Published <i>Without international search report and to be republished upon receipt of that report.</i> |
| (54) Title: SELF-GENERATION OF CERTIFICATES USING A SECURE MICROPROCESSOR IN A DEVICE FOR TRANSFERRING DIGITAL INFORMATION | | |
| (57) Abstract <p>Devices in a telecommunications system are provided with means to self-generate public key pairs and certificates. This eliminates the need for such keys and certificates to be sent to the devices from an outside source so a single-trust approach can be maintained. A manufacturer's certificate is installed into a device at the time of manufacture. The device only issues itself certificates based on a signed request from an external outside server. The device's self-issued certificates incorporate information obtained from the server in a profile. This allows control by the server over a device's self-issued certificates. In order to prevent tampering, and breaking, of the self-issued certificates, the certificate issuing process occurs within a secure microprocessor.</p> | | |

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

| | | | | | | | |
|----|--------------------------|----|--|----|--|----|--------------------------|
| AL | Albania | ES | Spain | LS | Lesotho | SI | Slovenia |
| AM | Armenia | FI | Finland | LT | Lithuania | SK | Slovakia |
| AT | Austria | FR | France | LU | Luxembourg | SN | Senegal |
| AU | Australia | GA | Gabon | LV | Latvia | SZ | Swaziland |
| AZ | Azerbaijan | GB | United Kingdom | MC | Monaco | TD | Chad |
| BA | Bosnia and Herzegovina | GE | Georgia | MD | Republic of Moldova | TG | Togo |
| BB | Barbados | GH | Ghana | MG | Madagascar | TJ | Tajikistan |
| BE | Belgium | GN | Guinea | MK | The former Yugoslav Republic of Macedonia | TM | Turkmenistan |
| BF | Burkina Faso | GR | Greece | | | TR | Turkey |
| BG | Bulgaria | HU | Hungary | ML | Mali | TT | Trinidad and Tobago |
| BJ | Benin | IE | Ireland | MN | Mongolia | UA | Ukraine |
| BR | Brazil | IL | Israel | MR | Mauritania | UG | Uganda |
| BY | Belarus | IS | Iceland | MW | Malawi | US | United States of America |
| CA | Canada | IT | Italy | MX | Mexico | UZ | Uzbekistan |
| CF | Central African Republic | JP | Japan | NE | Niger | VN | Viet Nam |
| CG | Congo | KE | Kenya | NL | Netherlands | YU | Yugoslavia |
| CH | Switzerland | KG | Kyrgyzstan | NO | Norway | ZW | Zimbabwe |
| CI | Côte d'Ivoire | KP | Democratic People's Republic of Korea | NZ | New Zealand | | |
| CM | Cameroon | | | PL | Poland | | |
| CN | China | KR | Republic of Korea | PT | Portugal | | |
| CU | Cuba | KZ | Kazakstan | RO | Romania | | |
| CZ | Czech Republic | LC | Saint Lucia | RU | Russian Federation | | |
| DE | Germany | LI | Liechtenstein | SD | Sudan | | |
| DK | Denmark | LK | Sri Lanka | SE | Sweden | | |
| EE | Estonia | LR | Liberia | SG | Singapore | | |

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
3 August 2000 (03.08.2000)

PCT

(10) International Publication Number
WO 00/45241 A3

(51) International Patent Classification⁷: **H04L 9/32,**
G06F 17/60

(21) International Application Number: **PCT/US00/02317**

(22) International Filing Date: **28 January 2000 (28.01.2000)**

(25) Filing Language: **English**

(26) Publication Language: **English**

(30) Priority Data:
60/117,788 29 January 1999 (29.01.1999) US
60/128,772 9 April 1999 (09.04.1999) US

(71) Applicant (for all designated States except US): **GENERAL INSTRUMENT CORPORATION [US/US]; 101 Tounament Drive, Horsham, PA 19044 (US).**

(72) Inventors; and

(75) Inventors/Applicants (for US only): **MEDVINSKY,**

Sasha [US/US]; 8873 Hampe Court, San Diego, CA 92129 (US). **SPRUNK, Eric, J. [US/US]; 6421 Cayenne Lane, Carlsbad, CA 92009 (US).**

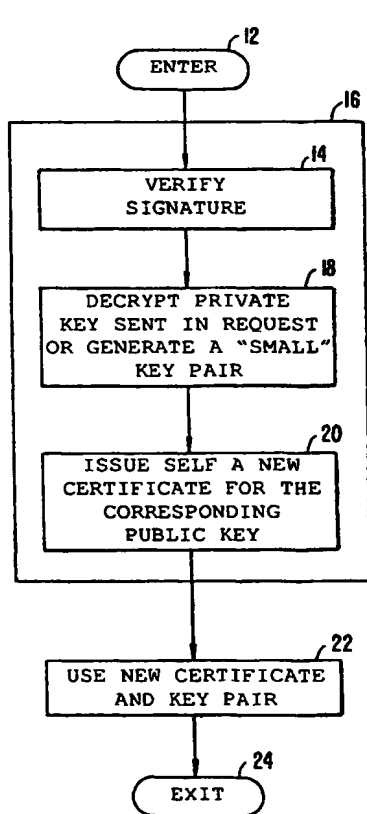
(74) Agents: **KULAS, Charles, J. et al.; Townsend and Townsend and Crew LLP, 8th floor, Two Embarcadero Center, San Francisco, CA 94111 (US).**

(81) Designated States (*national*): AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States (*regional*): ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU,

[Continued on next page]

(54) Title: **SELF-GENERATION OF CERTIFICATES USING A SECURE MICROPROCESSOR IN A DEVICE FOR TRANSFERRING DIGITAL INFORMATION**



(57) Abstract: The present invention allows consumer communications device in the figure such as an IP telephony adapter (110) to self-generate public key pairs (224) and certificates (214). This eliminates the need for such keys and certificates to be sent to the devices from an outside source so a single-trust approach can be maintained. A manufacturer's certificate is installed into a device at the time of manufacture. The device only issues itself certificates based on a signed request from an external outside server. The device's self-issued certificates incorporate information obtained from the server in a profile. This allows control by the server over a device's self-issued certificates. In order to prevent tampering, and breaking, of the self-issued certificates, the certificate issuing process occurs within a secure microprocessor.

WO 00/45241 A3

WO 00/45241 A3



MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

(88) Date of publication of the international search report:
14 December 2000

Published:

— With international search report.

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US00/02317

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) : H04L 9/32; G06F 17/60
US CL : 713/200, 201, 202; 709/303

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 713/200, 201, 202; 709/303

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

West search.
self-issuing certificate, generate certificate, encrypted public key, secure microprocessor, validity time.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|-----------|--|-----------------------|
| X,P | US 5,917,912 A (GINTER et al.) 29 JUNE 1999, col. 202, lines 3-41 and col.204 line 1 through col. 206 line 58. | 1 and 2 |
| A,E | US 6,058,188 A (CHANDERSEKARAN et al.) 02 MAY 2000, entire document. | 1-2 |
| A,E | US 6,026,491 A (HILES) 15 FEBRUARY 2000, entire document. | 1-2 |

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

| | |
|---|--|
| * Special categories of cited documents: | * later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention |
| *A* document defining the general state of the art which is not considered to be of particular relevance | *X* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone |
| *E* earlier document published on or after the international filing date | *Y* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art |
| *L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) | *Z* document member of the same patent family |
| *O* document referring to an oral disclosure, use, exhibition or other means | |
| *P* document published prior to the international filing date but later than the priority date claimed | |

Date of the actual completion of the international search

07 MAY 2000

Date of mailing of the international search report

15 AUG 2000

Name and mailing address of the ISA/US
Commissioner of Patents and Trademarks
Box PCT
Washington, D.C. 20231

Facsimile No. (703) 305-3230

Authorized officer

THOMAS C. LEE

Telephone No. (703) 305-9717